

Characterization of the strong divisibility property for generalized Fibonacci polynomials

Rigoberto Flórez

Department of Mathematics and Computer Science

The Citadel

Charleston, SC

U.S.A.

`rigo.florez@citadel.edu`

Robinson A. Higuera

Instituto de Matemáticas

Universidad de Antioquia

Medellín

Colombia

`robinson.higuera@udea.edu.co`

Antara Mukherjee

Department of Mathematics and Computer Science

The Citadel

Charleston, SC

U.S.A.

`antara.mukherjee@citadel.edu`

Abstract

It is known that the greatest common divisor of two Fibonacci numbers is again a Fibonacci number. It is called the *strong divisibility property*. However, this property does not hold for every second order sequence. In this paper we study the generalized Fibonacci polynomials and classify them in two types depending on their Binet formula. We give a complete characterization for those polynomials that satisfy the strong divisibility property. We also give formulas to calculate the gcd of those polynomials that do not satisfy the strong divisibility property.

1 Introduction

It is well known that the greatest common divisor (gcd) of two Fibonacci numbers is a Fibonacci number [18]. Thus, $\gcd(F_m, F_n) = F_{\gcd(m,n)}$. It is called the *strong divisibility*

property or *Fibonacci gcd property*. In this paper we study divisibility properties of generalized Fibonacci polynomials (GFP) and in particular we give characterization of the strong divisibility property for these polynomials.

We classify the GFP in two types, the Lucas type and the Fibonacci type, depending on their closed formulas or their Binet formulas (see for example, $L_n(x)$ (4) and $R_n(x)$ (6), and the Table 2). That is, if after solving the characteristic polynomial of the GFP we obtain a closed formula that look like the Binet formula for Fibonacci (Lucas) numbers, it is called Fibonacci (Lucas) type polynomials. Familiar examples of Fibonacci type polynomials are: Fibonacci polynomials, Pell polynomials, Fermat polynomials, Chebyshev polynomials of second kind, Jacobsthal polynomials and one type of Morgan-Voyce polynomials. Examples of Lucas type polynomials are: Lucas polynomials, Pell-Lucas polynomials, Fermat-Lucas polynomials, Chebyshev polynomials of first kind, Jacobsthal-Lucas polynomials and second type of Morgan-Voyce polynomials.

In Theorem 19 we prove that a GFP satisfies the strong divisibility property if and only if it is of Fibonacci type. The Theorem 15 shows that the Lucas type polynomials satisfy the strong divisibility property partially and also gives the *gcd* for those cases in which the property is not satisfied.

A Lucas type polynomial is equivalent to a Fibonacci type polynomial if they both have the same recurrence relation but different initial conditions (see also Flórez et al. [3]). The Theorem 18 proves that two equivalent GFP satisfies the strong divisibility property partially and gives the *gcd* for those cases in which the property is not satisfied.

In 1969 Webb and Parberry [26] extended the strong divisibility property to the Fibonacci Polynomials. In 1974 Hoggatt and Long [9] proved the strong divisibility property for one type of generalized Fibonacci polynomial. In 1978 Hoggatt and Bicknell-Johnson [10] extended the result mentioned in [9] to some cases of Fibonacci type polynomials. However, they did not prove the necessary and sufficient condition and their paper does not cover the Lucas type case. In 2005 Rayes, Trevisan, and Wang [23] proved that the strong divisibility property holds partially for the Chebyshev polynomials (we prove the general result in Theorem 15). Over the years several other authors have been also interested in the divisibility properties of sequences, some papers are [6, 12, 13, 14, 15, 20, 22, 25].

Lucas [15] proved the strong divisibility property (SDP) for Fibonacci numbers. However, the study of SDP for Lucas numbers took until 1991, when McDaniel [20] provided proofs that the Lucas numbers satisfy the SDP partially. In 1995 Hilton et al. [8] gave some more precise results about this property. As mentioned above several authors have been interested in the divisibility properties for Fibonacci type polynomials. However, the Lucas type polynomials have been less studied. Here we complete three cases of the SDP. Indeed, we give a characterization for the SDP for Fibonacci type polynomials and study both the SDP for Lucas type polynomials and the SDP for the combinations of Lucas type polynomials and Fibonacci type polynomials. Finally we provide an open question for the most general case of combination of two polynomials.

2 Generalized Fibonacci polynomials GFP

In the literature there are several definitions of generalized Fibonacci polynomials. However, the definition that we introduce here is simpler and covers other definitions. The background given in this section is a summary of the background given in [3]. However, the definition of generalized Fibonacci polynomial here is not exactly the same as in [3]. The *generalized Fibonacci polynomial* sequence, denoted by GFP, is defined by the recurrence relation

$$G_0(x) = p_0(x), G_1(x) = p_1(x), \text{ and } G_n(x) = d(x)G_{n-1}(x) + g(x)G_{n-2}(x) \text{ for } n \geq 2 \quad (1)$$

where $p_0(x)$ is a constant and $p_1(x)$, $d(x)$ and $g(x)$ are non-zero polynomials in $\mathbb{Z}[x]$ with $\gcd(d(x), g(x)) = 1$.

For example, if we let $p_0(x) = 0$, $p_1(x) = 1$, $d(x) = x$, and $g(x) = 1$ we obtain the regular Fibonacci polynomial sequence. Thus,

$$F_0(x) = 0, F_1(x) = 1, \text{ and } F_n(x) = xF_{n-1}(x) + F_{n-2}(x) \text{ for } n \geq 2.$$

Letting $x = 1$ and choosing the correct values for $p_0(x)$, $p_1(x)$, $d(x)$ and $g(x)$, the generalized Fibonacci polynomial sequence gives rise to three classical numerical sequences, the Fibonacci sequence, the Lucas sequence and the generalized Fibonacci sequence.

In Table 1 there are more familiar examples of GFP (see [3, 16, 17, 18]). Hoggatt and Bicknell-Johnson [10] show that Schechter polynomials are another example of generalized Fibonacci polynomials.

Polynomial	Initial value $G_0(x) = p_0(x)$	Initial value $G_1(x) = p_1(x)$	Recursive Formula $G_n(x) = d(x)G_{n-1}(x) + g(x)G_{n-2}(x)$
Fibonacci	0	1	$F_n(x) = xF_{n-1}(x) + F_{n-2}(x)$
Lucas	2	x	$D_n(x) = xD_{n-1}(x) + D_{n-2}(x)$
Pell	0	1	$P_n(x) = 2xP_{n-1}(x) + P_{n-2}(x)$
Pell-Lucas	2	$2x$	$Q_n(x) = 2xQ_{n-1}(x) + Q_{n-2}(x)$
Pell-Lucas-prime	1	x	$Q'_n(x) = 2xQ'_{n-1}(x) + Q'_{n-2}(x)$
Fermat	0	1	$\Phi_n(x) = 3x\Phi_{n-1}(x) - 2\Phi_{n-2}(x)$
Fermat-Lucas	2	$3x$	$\vartheta_n(x) = 3x\vartheta_{n-1}(x) - 2\vartheta_{n-2}(x)$
Chebyshev second kind	0	1	$U_n(x) = 2xU_{n-1}(x) - U_{n-2}(x)$
Chebyshev first kind	1	x	$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x)$
Jacobsthal	0	1	$J_n(x) = J_{n-1}(x) + 2xJ_{n-2}(x)$
Jacobsthal-Lucas	2	1	$j_n(x) = j_{n-1}(x) + 2xj_{n-2}(x)$
Morgan-Voyce	0	1	$B_n(x) = (x+2)B_{n-1}(x) - B_{n-2}(x)$
Morgan-Voyce	2	$x+2$	$C_n(x) = (x+2)C_{n-1}(x) - C_{n-2}(x)$

Table 1: Recurrence relation of some GFP.

2.1 Fibonacci type and Lucas type polynomials

If we impose some conditions on the Definition (1) we obtain two type of distinguishable polynomials. We say that a sequences as in (1) is *Lucas type* or *first type* if $2p_1(x) = p_0(x)d(x)$

with $p_0 \neq 0$. We say that a sequences as in (1) is *Fibonacci type* or *second type* if $p_0(x) = 0$ with $p_1(x)$ a constant.

If $d^2(x) + 4g(x) > 0$, then the explicit formula for the recurrence relation (1) is given by

$$G_n(x) = t_1 a^n + t_2 b^n \quad (2)$$

where $a(x)$ and $b(x)$ are the solutions of the quadratic equation associated to the second order recurrence relation $G_n(x)$. That is, $a(x)$ and $b(x)$ are the solutions of $z^2 - d(x)z - g(x) = 0$. The explicit formula for $G_n(x)$ given in (2) with $G_0(x) = p_0(x)$ and $G_1(x) = p_1(x)$ imply that

$$t_1 = \frac{p_1(x) - p_0(x)b(x)}{a(x) - b(x)} \text{ and } t_2 = \frac{-p_1(x) + p_0(x)a(x)}{a(x) - b(x)} \quad (3)$$

Using (2) and (3) we obtain the Binet formulas for the Generalized Fibonacci sequences of the Lucas type and Fibonacci type. Thus, substituting $2p_1(x) = p_0(x)d(x)$ in (3) we obtain that $t_1 = t_2 = p_0(x)/2$. Substituting this in (2) and letting α be $2/p_0(x)$ we obtain the Binet formula for Generalized Fibonacci sequence of *Lucas type* or *first type*

$$L_n(x) = \frac{a^n(x) + b^n(x)}{\alpha}. \quad (4)$$

We want α be an integer, therefore $|p_0(x)| = 1$ or 2 .

Now, substituting $p_0(x) = 0$ and the constant $p_1(x)$ in (3) we obtain that $t_1 = t_2 = p_1(x)$. Substituting this in (2) we obtain the Binet formula for Generalized Fibonacci sequence of *Fibonacci type* or *second type*

$$R_n(x) = \frac{p_1(x)(a^n(x) - b^n(x))}{a(x) - b(x)}. \quad (5)$$

In this paper we are interested only on $R_n(x)$ when $p_1(x) = 1$. Therefore, the Binet formula $R_n(x)$ that we use here is

$$R_n(x) = \frac{a^n(x) - b^n(x)}{a(x) - b(x)}. \quad (6)$$

Note that $a(x) + b(x) = d(x)$, $a(x)b(x) = -g(x)$ and $a(x) - b(x) = \sqrt{d^2(x) + 4g(x)}$ where $d(x)$ and $g(x)$ are the polynomials defined on the generalized Fibonacci polynomials.

A generalized Fibonacci polynomial which satisfies the Binet formula (4) is said to be of *first type* or *Lucas type* and it is of *Second type* or *Fibonacci type* if it satisfies the Binet formula (6). Horadam [11] and André-Jeannin [1] have studied these polynomials in detail.

The sequence of polynomials that have Binet representations $R_n(x)$ or $L_n(x)$ depend only on $d(x)$ and $g(x)$ defined on the generalized Fibonacci polynomials. We say that a generalized Fibonacci sequence of Lucas (Fibonacci) type is *equivalent* to a sequence of the Fibonacci (Lucas) type, if their recursive sequences are determined by the same polynomials $d(x)$ and $g(x)$. Notice that two equivalent polynomials have the same $a(x)$ and $b(x)$ in their Binet representations.

For example, the Lucas polynomial is a GFP of Lucas type, whereas the Fibonacci polynomial is a GFP of Fibonacci type. Lucas and Fibonacci polynomials are equivalent because $d(x) = x$ and $g(x) = 1$ (see Table 1). Note that in their Binet representations they

both have $a(x) = (x + \sqrt{x^2 + 4})/2$ and $b(x) = (x - \sqrt{x^2 + 4})/2$. The Table 2 is based on information from the following papers [1, 3, 11]. The leftmost polynomials in Table 2 are of the Lucas type and their equivalent polynomials are in the third column on the same line. In the last two columns of Table 2 we can see the $a(x)$ and $b(x)$ that the pairs of equivalent polynomials share. It is easy to obtain the characteristic equations of the sequences given in Table 1, and the roots of the equations are $a(x)$ and $b(x)$.

For the sake of simplicity throughout this paper we use a in place of $a(x)$ and b in place of $b(x)$ when they appear in the Binet formulas. We use the notation G_n^* or G_n' for G_n depending on when it satisfies the Binet formulas (4) or (6), respectively, (see Section 4).

For most of the proofs of GFP of Lucas type it is required that $\gcd(p_0(x), p_1(x)) = 1$, $\gcd(p_0(x), d(x)) = 1$ and $\gcd(d(x), g(x)) = 1$. It is easy to see that $\gcd(\alpha, G_n^*(x)) = 1$. Therefore, for the rest the paper we suppose that these four mentioned conditions hold for all generalized Fibonacci polynomial sequences of Lucas type treated here. We use ρ to denote $\gcd(d(x), G_1(x))$. Notice that in the definition Pell-Lucas we have that $p_0(x) = 2$ and $p_1(x) = 2x$. Thus, the $\gcd(p_0(x), p_1(x)) \neq 1$. Therefore, Pell-Lucas does not satisfy the extra conditions that were just imposed for Generalized Fibonacci polynomial. To solve this problem we define *Pell-Lucas-prime* as follows:

$$Q'_0(x) = 1, Q'_1(x) = x, \text{ and } Q'_n(x) = 2xQ'_{n-1}(x) + Q'_{n-2}(x) \text{ for } n \geq 2.$$

It easy to see that $2Q'_n(x) = Q_n(x)$ and that $\alpha = 2$. Flórez, Junes and Higuita [4] worked similar problems for numerical sequences.

Note. The definition of Generalized Fibonacci Polynomial in [3] differs with definition on this papers due to the initial conditions on the Fibonacci type polynomials. Thus, the initial conditions for the Fibonacci type polynomials in [3] is $G_0(x) = p_0(x) = 1$ and so implicitly $G_{-1}(x) = 0$. However, our definition for the Lucas type polynomials are the same in both papers.

Polynomial Lucas type	$L_n(x)$	Polynomial of Fibonacci type	$R_n(x)$	$a(x)$	$b(x)$
Lucas	$D_n(x)$	Fibonacci	$F_n(x)$	$(x + \sqrt{x^2 + 4})/2$	$(x - \sqrt{x^2 + 4})/2$
Pell-Lucas-prime	$Q'_n(x)$	Pell	$P_n(x)$	$x + \sqrt{x^2 + 1}$	$x - \sqrt{x^2 + 1}$
Fermat-Lucas	$\vartheta_n(x)$	Fermat	$\Phi_n(x)$	$(3x + \sqrt{9x^2 - 8})/2$	$(3x - \sqrt{9x^2 - 8})/2$
Chebyshev first kind	$T_n(x)$	Chebyshev second kind	$U_n(x)$	$x + \sqrt{x^2 - 1}$	$x - \sqrt{x^2 - 1}$
Jacobsthal-Lucas	$j_n(x)$	Jacobsthal	$J_n(x)$	$(1 + \sqrt{1 + 8x})/2$	$(1 - \sqrt{1 + 8x})/2$
Morgan-Voyce	$C_n(x)$	Morgan-Voyce	$B_n(x)$	$(x + 2 + \sqrt{x^2 + 4x})/2$	$(x + 2 - \sqrt{x^2 + 4x})/2$

Table 2: $R_n(x)$ equivalent to $L_n(x)$.

3 Divisibility properties of Generalized Fibonacci Polynomials

In this section we prove a few divisibility and gcd properties which are true for all GFP. These results will be used in a section later on to prove the main results of this paper.

Proposition 1 parts (1) and (2) is a generalization of Proposition 2.2 in [5]. The proof here is similar the proof in [5] since both use properties of integral domains. The reader can therefore update the proof in the afore-mentioned paper to obtain the proof of this proposition.

Proposition 1. *Let $p(x), q(x), r(x)$, and $s(x)$ be polynomials.*

(1) *If $\gcd(p(x), q(x)) = \gcd(r(x), s(x)) = 1$, then*

$$\gcd(p(x)q(x), r(x)s(x)) = \gcd(p(x), r(x)) \gcd(p(x), s(x)) \gcd(q(x), r(x)) \gcd(q(x), s(x)).$$

(2) *If $\gcd(p(x), r(x)) = 1$ $\gcd(q(x), s(x)) = 1$, then*

$$\gcd(p(x)q(x), r(x)s(x)) = \gcd(p(x), s(x)) \gcd(q(x), r(x)).$$

(3) *If $z_1(x) = \gcd(p(x), r(x))$ and $z_2(x) = \gcd(q(x), s(x))$, then*

$$\gcd(p(x)q(x), r(x)s(x)) = \frac{\gcd(z_2(x)p(x), z_1(x)s(x)) \gcd(z_1(x)q(x), z_2(x)r(x))}{z_1(x)z_2(x)}.$$

Proof. We prove part (3). Since $\gcd(p(x), r(x)) = z_1(x)$ and $\gcd(q(x), s(x)) = z_2(x)$, there are polynomials $P(x), S(x), Q(x)$ and $R(x)$ with $\gcd(P(x), R(x)) = \gcd(Q(x), S(x)) = 1$, such that $p(x) = z_1(x)P(x)$, $s(x) = z_2(x)S(x)$, $r(x) = z_1(x)R(x)$, $q(x) = z_2(x)Q(x)$. So,

$$\begin{aligned} \gcd(p(x)q(x), r(x)s(x)) &= \gcd(z_1(x)P(x)z_2(x)Q(x), z_1(x)R(x)z_2(x)S(x)) \\ &= z_1(x)z_2(x) \gcd(P(x)Q(x), R(x)S(x)). \end{aligned}$$

From part (2) we know that $\gcd(P(x)Q(x), R(x)S(x)) = \gcd(P(x), S(x)) \gcd(Q(x), R(x))$. Now it is easy to see that

$$\gcd(p(x)q(x), r(x)s(x)) = \frac{\gcd(z_2(x)p(x), z_1(x)s(x)) \gcd(z_1(x)q(x), z_2(x)r(x))}{z_1(x)z_2(x)}.$$

This proves part (3). □

We recall that $\rho = \gcd(d(x), G_1(x))$ and that for GFP of Lucas type it is required that $\gcd(p_0(x), p_1(x)) = 1$, $\gcd(p_0(x), d(x)) = 1$, $\gcd(p_0(x), g(x)) = 1$ and $\gcd(d(x), g(x)) = 1$. We also recall $p_0(x) = 0$ and $p_1(x) = 1$ for GFP of Fibonacci type.

For the rest of the paper we use the notation G_n^* if the generalized Fibonacci polynomial G_n satisfies the Binet formula (4) and G_n' if the generalized Fibonacci polynomial G_n satisfies the Binet formula (6). We use G_n if the result does not need the mentioned classification to be true. We recall that for Lucas type polynomials $|p_0(x)| = 1$ or 2 and for Fibonacci type polynomial $p_1(x) = 1$.

Lemma 2. *If $\{G_n(x)\}$ is a GFP of either Lucas or Fibonacci type, then*

- (1) $\gcd(d(x), G_{2n+1}(x)) = G_1(x)$ for every positive integer n ,
- (2) If the GFP is of Lucas type, then $\gcd(d(x), G_{2n}^*(x)) = 1$ and
if the GFP is of Fibonacci type, then $\gcd(d(x), G_{2n}'(x)) = d(x)$
- (3) $\gcd(g(x), G_n(x)) = \gcd(g(x), G_1(x)) = 1$, for every positive integer n .

Proof. We prove part (1) by induction, the proof of part (2) is similar and we omit it.

Let $\{G_n\}$ a GFP. Let $S(n)$ be the statement

$$\rho = \gcd(d(x), G_{2n+1}(x)) \text{ for } n \geq 1.$$

To prove $S(1)$ we suppose that $\gcd(d(x), G_3(x)) = r$. Thus, r divides any linear combination of $d(x)$ and $G_3(x)$. Therefore, r divides $G_3(x) - d(x)G_2(x)$. This and given that $G_3(x) = d(x)G_2(x) + g(x)G_1(x)$, imply that $r \mid g(x)G_1(x)$. So, $r \mid \gcd(d(x), g(x)G_1(x))$. Since $\gcd(d(x), g(x)) = 1$, we have that $r \mid \rho$. It is easy to see that $\rho \mid r$. Thus, $r = \gcd(d(x), G_1(x))$. This proves $S(1)$.

We suppose that $S(n)$ is true for $n = k - 1$. That is, suppose that $\gcd(d(x), G_{2k-1}(x)) = \rho$. To prove $S(k)$ we suppose that $\gcd(d(x), G_{2k+1}(x)) = r'$. Thus, r' divides any linear combination of $d(x)$ and $G_{2k+1}(x)$. Therefore, r' divides $G_{2k+1}(x) - d(x)G_{2k}(x)$. This and given that $G_{2k+1}(x) = d(x)G_{2k}(x) + g(x)G_{2k-1}(x)$, imply that $r' \mid g(x)G_{2k-1}(x)$. Therefore, $r' \mid \gcd(d(x), g(x)G_{2k-1}(x))$. Since $\gcd(d(x), g(x)) = 1$, we have that $r' \mid \gcd(d(x), G_{2k-1}(x))$. By the inductive hypothesis we know that $\gcd(d(x), G_{2k-1}(x)) = \rho$. Thus, $r' \mid \rho$. It is easy to see that $\gcd(d(x), G_{2k+1}(x))$ divides r' . So, $r' = \gcd(G_1(x), d(x))$.

We now show that depending on the type of the sequence it holds that $\gcd(d(x), G_1(x)) = G_1$. If $\{G_n(x)\}$ is a GFP of Fibonacci type, by definition of $p(x)$ we that $G_1(x) = 1$ (see comments after Binet formula (5)). Suppose that $\{G_n(x)\}$ is a GFP of Lucas type. Recall that $2p_1(x) = p_0(x)d(x)$ and that $|p_0(x)| = 1$ or 2 . The conclusion is straightforward since $G_1(x) = (a(x) + b(x))/\alpha = d(x)/\alpha$.

Proof of part (2). Let $S(n)$ be the statement

$$\rho = \gcd(d(x), G_{2n}(x)) \text{ for } n \geq 1.$$

To prove $S(2)$ we suppose that $\gcd(d(x), G_4(x)) = r$. Thus, r divides any linear combination of $d(x)$ and $G_4(x)$. Therefore, r divides $G_4(x) - d(x)G_3(x)$. This and given that $G_4(x) = d(x)G_3(x) + g(x)G_2(x)$, imply that $r \mid g(x)G_2(x)$. Therefore, $r \mid \gcd(d(x), g(x)G_2(x))$. Since $\gcd(d(x), g(x)) = 1$, we have that $r \mid \rho$. It is easy to see that $\rho \mid r$. Thus, $r = \gcd(d(x), G_2(x))$. This proves $S(2)$.

We suppose that $S(n)$ is true for $n = k - 1$. That is, suppose that $\gcd(d(x), G_{2k-2}(x)) = \rho$. To prove $S(k)$ we suppose that $\gcd(d(x), G_{2k}(x)) = r'$. Thus, r' divides any linear combination of $d(x)$ and $G_{2k}(x)$. Therefore, r' divides $G_{2k}(x) - d(x)G_{2k-1}(x)$. This and given that $G_{2k}(x) = d(x)G_{2k-1}(x) + g(x)G_{2k-2}(x)$, imply that $r' \mid g(x)G_{2k-2}(x)$. Therefore, $r' \mid \gcd(d(x), g(x)G_{2k-2}(x))$. Since $\gcd(d(x), g(x)) = 1$, we have that $r' \mid \gcd(d(x), G_{2k-2}(x))$. By the inductive hypothesis we know that $\gcd(d(x), G_{2k-2}(x)) = \rho$. Thus, $r' \mid \rho$. It is easy to see that $\gcd(d(x), G_{2k}(x))$ divides r' . So, $r' = \gcd(G_2(x), d(x))$.

We observe that for a GFP of Fibonacci type it holds that $G'_2(x) = a(x) + b(x) = d(x)$. So, it is clear that $\gcd(G'_{2n}(x), d(x)) = d(x)$. For a GFP of Lucas type it holds that $G_0^*(x)$ is a non-zero constant. Since $G_2^*(x) = d(x)G_1^*(x) + G_0^*g(x)$, and $\gcd(d(x), g(x)) = 1$, we have

$$\gcd(d(x), G_2^*(x)) = \gcd(d(x), d(x)G_1^*(x) + G_0^*g(x)) = \gcd(d(x), G_0^*(x)g(x)) = 1.$$

Proof of part (3). We now prove that $\gcd(g(x), G_1(x)) = 1$ by cases. If $G_1(x)$ is of the Fibonacci type, the conclusion is straightforward. As a second case we suppose that $G_1(x)$ is of the Lucas type. That is $G_1(x)$ satisfies the Binet formula (4). Therefore, we have that

$$\gcd(g(x), G_1(x)) = \gcd(g(x), L_1(x)) = \gcd(g(x), [a + b]/\alpha) = \gcd(g(x), d(x)/\alpha).$$

Since $\gcd(g(x), d(x)) = 1$, we have that $\gcd(g(x), d(x)/\alpha) = 1$. This completes the proof. \square

Lemma 3. *If $\{G_n(x)\}$ is a GFP polynomial sequence, then for every positive integer n it holds that*

$$(1) \gcd(G_n(x), G_{n+1}(x)) \text{ divides } \gcd(G_n(x), g(x)G_{n-1}(x)) = \gcd(G_n(x), G_{n-1}(x)),$$

$$(2) \gcd(G_n(x), G_{n+2}(x)) \text{ divides } \gcd(G_n(x), d(x)G_{n+1}(x)).$$

Proof. We prove part (1), the proof of part (2) is similar and we omit it. If r is equal to $\gcd(G_n(x), G_{n+1}(x))$, then r divides any linear combination of $G_n(x)$ and $G_{n+1}(x)$. Therefore, $r \mid (G_{n+1}(x) - d(x)G_n(x))$. This and the recursive definition of $G_{n+1}(x)$ imply that $r \mid g(x)G_{n-1}(x)$. Therefore, $r \mid \gcd(g(x)G_{n-1}(x), G_n(x))$. Since $\gcd(g(x), G_n(x)) = 1$, we have that $\gcd(g(x)G_{n-1}(x), G_n(x)) = \gcd(G_{n-1}(x), G_n(x))$. This completes the proof. \square

Proposition 4. *Let m and n be positive integers with $0 < |m - n| \leq 2$.*

(1) *If $\{G_t^*(x)\}$ is a GFP of Lucas type, then*

$$\gcd(G_m^*(x), G_n^*(x)) = \begin{cases} G_1^*(x), & \text{if } m \text{ and } n \text{ are both odd;} \\ 1, & \text{otherwise.} \end{cases}$$

(2) *If $\{G'_t(x)\}$ is a GFP of Fibonacci type, then*

$$\gcd(G'_m(x), G'_n(x)) = \begin{cases} G'_2(x) & \text{if } m \text{ and } n \text{ are both even;} \\ 1, & \text{otherwise.} \end{cases}$$

Proof. We prove part (1) using several cases based on the values of m and n . The proof of part (2) is similar and we omit. We first provide the proof for the case when m and n are consecutive integers using induction on m . Let $S(m)$ be the statement

$$\gcd(G_m^*(x), G_{m+1}^*(x)) = 1 \text{ for } m \geq 1.$$

First we prove $S(1)$. From Lemma 3 part (1), we know that

$$\gcd(G_1^*(x), G_2^*(x)) \text{ divides } \gcd(G_1^*(x), g(x)G_0^*(x)). \quad (7)$$

Since

$$\gcd(G_0^*(x), G_1^*(x)) = \gcd(p_0(x), p_1(x)) = 1,$$

we have that

$$\gcd(G_1^*(x), g(x)G_0^*(x)) = \gcd(G_1^*(x), g(x)).$$

This, (7) and Lemma 2 part (3) imply that $\gcd(G_1^*(x), G_2^*(x)) = 1$.

We suppose that $S(m)$ is true for $m = k-1$. Thus, suppose that $\gcd(G_{k-1}^*(x), G_k^*(x)) = 1$. We prove that $S(k)$ is true. From Lemma 3 part (1), we know that

$$\gcd(G_k^*(x), G_{k+1}^*(x)) \text{ divides } \gcd(G_k^*(x), g(x)G_{k-1}^*(x)). \quad (8)$$

From Lemma 2 part (3) we know that $\gcd(G_k^*(x), g(x)) = 1$. So,

$$\gcd(G_k^*(x), g(x)G_{k-1}^*(x)) = \gcd(G_k^*(x), G_{k-1}^*(x)).$$

This, (8) and the inductive hypothesis imply that $\gcd(G_k^*(x), G_{k+1}^*(x)) = 1$.

We now prove the proposition for consecutive even integers (this proof is actually a direct consequence of the previous proof). From Lemma 3 part (2), we have $\gcd(G_{2k}^*(x), G_{2k+2}^*(x))$ divides $\gcd(G_{2k}^*(x), d(x)G_{2k+1}^*(x))$. From Lemma 2 part (2) we know that $\gcd(d(x), G_{2k}^*(x)) = 1$. This implies that $\gcd(G_{2k}^*(x), d(x)G_{2k+1}^*(x)) = \gcd(G_{2k}^*(x), G_{2k+1}^*(x))$. From the previous part—that is, the case when m and n are consecutive integers—of this proof we conclude that $\gcd(G_{2k}^*(x), G_{2k+1}^*(x)) = 1$. This proves that $\gcd(G_{2k}^*(x), G_{2k+2}^*(x)) = 1$.

Finally we prove the proposition for consecutive odd integers. From the recursive definition of GFP we have that $\gcd(G_{2k+1}^*(x), G_{2k-1}^*(x))$ equals

$$\gcd(d(x)G_{2k}^*(x) + g(x)G_{2k-1}^*(x), G_{2k-1}^*(x)) = \gcd(d(x)G_{2k}^*(x), G_{2k-1}^*(x))$$

From the first case in this proof we know that $\gcd(G_{2k}^*(x), G_{2k-1}^*(x)) = 1$. This implies that $\gcd(G_{2k+1}^*(x), G_{2k-1}^*(x)) = \gcd(d(x), G_{2k-1}^*(x))$. This and Lemma 2 imply that

$$\gcd(G_{2k+1}^*(x), G_{2k-1}^*(x)) = \gcd(d(x), G_{2k-1}^*(x)) = G_1^*(x).$$

This completes the proof of part (1). \square

4 Identities and other properties of Generalized Fibonacci Polynomials

In this section we present some identities that the GFP satisfy. These identities are required for the proofs of certain divisibility properties of the GFP. The results in this section are proved using the Binet formulas (see Section 2). Proposition 5 part (1) is a variation of a result proved by Hoggatt and Long [9], similarly Proposition 8 is a variation of a divisibility property proved by them in the same paper.

In 1963 Ruggles [18] proved that $F_{n+m} = F_n L_m - (-1)^m F_{n-m}$. Proposition 5 parts (2) and (3) are a generalization of this numerical identity. In 1972 Hansen [7] proved that $5F_{m+n-1} = L_m L_n + L_{m-1} L_{n-1}$. Proposition 6 part (1) is a generalization of this numerical identity.

Proposition 5. *If $\{G_n^*(x)\}$ and $\{G'_n(x)\}$ are equivalent GFP sequences, then*

- (1) $G'_{m+n+1}(x) = G'_{m+1}(x)G'_{n+1}(x) + g(x)G'_m(x)G'_n(x),$
- (2) *if $n \geq m$, then $G'_{n+m}(x) = \alpha G'_n(x)G_m^*(x) - (-g(x))^m G'_{n-m}(x),$*
- (3) *if $n \geq m$, then $G'_{n+m}(x) = \alpha G'_m(x)G_n^*(x) + (-g(x))^m G'_{n-m}(x).$*

Proof. We prove part (1). We know that $\{G'_n(x)\}$ satisfies the Binet formula (6). That is, $R_n(x) = (a^n - b^n)/(a - b)$. (Recall that we use $a := a(x)$ and $b := b(x)$.)

Therefore, $G'_{m+1}(x)G'_{n+1}(x) + g(x)G'_m(x)G'_n(x)$ is equal to,

$$[(a^{m+1} - b^{m+1})(a^{n+1} - b^{n+1}) + g(x)(a^m - b^m)(a^n - b^n)] / (a - b)^2.$$

Simplifying and factoring terms we obtain,

$$[(a^{n+m}(a^2 + g(x)) + b^{n+m}(b^2 + g(x))) - (a^n b^m + b^n a^m)(ab + g(x))] / (a - b)^2.$$

Next, since $ab = -g(x)$, we see that the above expression is equal to,

$$[a^{n+m}(a^2 + g(x)) + b^{n+m}(b^2 + g(x))] / (a - b)^2.$$

This, with the facts that, $(a^2 + g(x)) = a(a - b)$ and $(b^2 + g(x)) = -b(a - b)$, shows that the above expression is equal to

$$(a^{n+m+1} - b^{n+m+1}) / (a - b) = R_{n+m+1}(x).$$

We prove part (2) the proof of part (3) is identical and we omit it. Suppose that $G_k^*(x)$ is equivalent to $G'_k(x)$ and that $G_k^*(x)$ is of the Lucas type for all k . For simplicity let us suppose that $\alpha = 1$ (the proof when $\alpha \neq 1$ is similar, so we omit it). Using the Binet formulas (4) and (6) we obtain that $G'_n(x)G_m^*(x) - (-g(x))^m G'_{n-m}(x)$ equals

$$\frac{(a^n - b^n)(a^m + b^m) - (-g(x))^m(a^{n-m} - b^{n-m})}{(a - b)}.$$

After performing the indicated multiplication and simplifying we obtain that this expression is equal to

$$\left[\frac{a^{n+m} - b^{n+m}}{a - b} \right] + \left[\frac{a^n b^m - a^m b^n - (-g(x))^m a^{n-m} + (-g(x))^m b^{n-m}}{a - b} \right].$$

Since $-g(x) = ab$, it is easy to see that the expression in the right bracket is equal to zero. Thus, $(a^{n+m} - b^{n+m})/(a - b) = G'_{n+m}(x)$. This completes the proof of part (2). \square

Proposition 6. *Let $\{G_n^*(x)\}$ and $\{G'_n(x)\}$ be equivalent GFP sequences. If $m \geq 0$ and $n \geq 0$, then*

- (1) $(a - b)^2 G'_{m+n+1}(x) = \alpha^2 G_{m+1}^*(x)G_{n+1}^*(x) + \alpha^2 g(x)G_m^*(x)G_n^*(x),$

$$(2) \quad G_{m+n+2}^*(x) = \alpha G_{m+1}^*(x) G_{n+1}^*(x) + g(x) [\alpha G_m^*(x) G_n^*(x) - G_{m+n}^*(x)].$$

Proof. In this proof we use $\alpha = 1$, the proof when $\alpha \neq 1$ is similar, so we omit it. (Recall, once again, that we use $a := a(x)$ and $b := b(x)$.)

Proof of part (1). Since $G_n^*(x)$ is a Fibonacci polynomial of the Lucas type, we have that $G_n^*(x)$ satisfies the Binet formula $L_n(x) = (a^n + b^n)/\alpha$ given in (4). Therefore,

$$G_{m+1}^*(x) G_{n+1}^*(x) + g(x) G_m^*(x) G_n^*(x) \quad (9)$$

is equal to,

$$[a^{n+1} + b^{n+1}] [a^{m+1} + b^{m+1}] + g(x) [a^n + b^n] [a^m + b^m].$$

Simplifying and factoring we see that this expression is equal to

$$a^{m+n} [a^2 + g(x)] + b^{m+n} [b^2 + g(x)] + (ab + g(x)) [a^m b^n + a^n b^m].$$

Since

$$ab = -g(x), \quad a^2 + g(x) = a(a - b), \quad \text{and} \quad b^2 + g(x) = -b(a - b),$$

we have that the expression in (9) is equal to $(a - b)(a^{m+n+1} - b^{m+n+1})$. We recall that $G'_{m+n+1}(x)$ is equivalent to $G_{m+n+1}^*(x)$. Thus, $G'_{m+n+1}(x) = (a^{m+n+1} - b^{m+n+1})/(a - b)$. Therefore, $(a - b)^2 G'_{m+n+1}(x) = (a - b) [a^{m+n+1} - b^{m+n+1}]$. This completes the proof of part (1).

Proof of part (2). From the proof of part (1) we know that

$$(a - b)^2 G'_{m+n+1}(x) = (a - b) [a^{m+n+1} - b^{m+n+1}].$$

Simplifying the right side of the previous equality we have that

$$(a - b)^2 G'_{m+n+1}(x) = a^{m+n+2} - ba^{m+n+1} - ab^{m+n+1} + b^{m+n+2}.$$

So, $(a - b)^2 G'_{m+n+1}(x) = a^{m+n+2} + b^{m+n+2} - ab[a^{m+n} + b^{m+n}]$. We recall that $ab = -g(x)$. Thus,

$$(a - b)^2 G'_{m+n+1}(x) = a^{m+n+2} + b^{m+n+2} + g(x) [a^{m+n} + b^{m+n}].$$

This and the Binet formula (4), imply that

$$(a - b)^2 G'_{m+n+1}(x) = G_{m+n+2}^*(x) + g(x) G_{m+n}^*(x).$$

So, the proof follows from part (1) of this Proposition. \square

Proposition 7. Let $\{G_n^*(x)\}$ be a GFP sequence of the Lucas type. If m, n, r , and q are positive integers, then

$$(1) \quad \text{if } m \leq n, \text{ then } G_{m+n}^*(x) = \alpha G_m^*(x) G_n^*(x) + (-1)^{m+1} (g(x))^m G_{n-m}^*(x),$$

$$(2) \quad \text{if } r < m, \text{ then there is a polynomial } T(x) \text{ such that}$$

$$G_{mq+r}^*(x) = \begin{cases} G_m^*(x) T(x) + (-1)^{m(t-1)+t+r} (g(x))^{(t-1)m+r} G_{m-r}^*(x), & \text{if } q \text{ is odd;} \\ G_m^*(x) T(x) + (-1)^{(m+1)t} (g(x))^{mt} G_r^*(x), & \text{if } q \text{ is even} \end{cases}$$

$$\text{where } t = \left\lceil \frac{q}{2} \right\rceil,$$

(3) if $n > 1$, then there is a polynomial $T_n(x)$ such that

$$G_{2n_r}^*(x) = G_r^*(x)T_n(x) + (2/\alpha)(g(x))^{2^{n-1}r}.$$

Proof. We prove part (1). Since $G_m^*(x)$ and $G_n^*(x)$ are of the Lucas type, they both satisfy the Binet formula (4). Thus,

$$G_m^*(x)G_n^*(x) = \left(\frac{a^m + b^m}{\alpha}\right) \left(\frac{a^n + b^n}{\alpha}\right) = \frac{a^{m+n} + b^{m+n}}{\alpha^2} + \frac{(ab)^m(a^{n-m} + b^{n-m})}{\alpha^2}.$$

So, $G_m^*(x)G_n^*(x) = [G_{n+m}^*(x) + (ab)^m G_{n-m}^*(x)] / \alpha$. This and $ab = -g(x)$, imply that

$$G_{m+n}^*(x) = \alpha G_m^*(x)G_n^*(x) - (-g(x))^m G_{n-m}^*(x).$$

This completes the proof of part (1).

We first prove part (2) when q is odd by induction. Suppose $q = 2t - 1$, and let $S(t)$ be the following statement. For every positive integer t there is a polynomial $T_t(x)$ such that

$$G_{m(2t-1)+r}^*(x) = G_m^*(x)T_t(x) + (-1)^{m(t-1)+t+r}(g(x))^{(t-1)m+r}G_{m-r}^*(x).$$

From part (1), taking $T_1(x) = \alpha G_r^*(x)$, it is easy to see that $S(t)$ is true if $t = 1$.

We suppose that $S(k)$ is true. That is, suppose that there is a polynomial $T_k(x)$ such that

$$G_{m(2k-1)+r}^*(x) = G_m^*(x)T_k(x) + (-1)^{m(k-1)+t+r}(g(x))^{(k-1)m+r}G_{m-r}^*(x). \quad (10)$$

We prove that $S(k+1)$ is true. Notice that $G_{m(2k+1)+r}^*(x) = G_{(2km+r)+m}^*(x)$. Therefore, from part (1) we have

$$G_{m(2k+1)+r}^*(x) = \alpha G_m^*(x)G_{2km+r}^*(x) + (-1)^{m+1}g^m(x)G_{m(2k-1)+r}^*(x).$$

This and $S(k)$ (see (10)), imply that $G_{m(2k+1)+r}^*(x)$ equals

$$\alpha G_m^*(x)G_{2km+r}^*(x) + (-1)^{m+1}(g(x))^m G_m^*(x)T_k(x) + (-1)^{km+(t+1)+r}(g(x))^{km+r}G_{m-r}^*(x).$$

Therefore, $G_{m(2k+1)+r}^*(x)$ equals

$$G_m^*(x)[\alpha G_{2km+r}^*(x) + (-1)^{m+1}(g(x))^m T_k(x)] + (-1)^{km+(t+1)+r}(g(x))^{km+r}G_{m-r}^*(x).$$

This, with $T_{k+1}(x) := \alpha G_{2km+r}^*(x) + (-1)^{m+1}(g(x))^m T_k(x)$, implies $S(k+1)$. This complete the proof when q is odd.

We now prove part (2) when q is even by induction –this proof is similar to the case when q is odd–. Suppose $q = 2t$, and let $H(t)$ be the following statement. For every positive integer number there is a polynomial $T_t(x)$ such that

$$G_{m(2t)+r}^*(x) = G_m^*(x)T_t(x) + (-1)^{(m+1)t}(g(x))^{mt}G_r^*(x).$$

From part (1), taking $T_1(x) = \alpha G_r^*(x)$, it is easy to see that $H(t)$ is true if $t = 1$.

We suppose that $H(k)$ is true. That is, suppose that there is a polynomial $T_k(x)$ such that

$$G_{m(2k)+r}^*(x) = G_m^*(x)T_k(x) + (-1)^{(m+1)k}(g(x))^{mk}G_r^*(x). \quad (11)$$

We prove that $H(k+1)$ is true. Notice that $G_{2m(k+1)+r}^*(x) = G_{((2k+1)m+r)+m}^*(x)$. Therefore, from part (1) we have that

$$G_{2m(k+1)+r}^*(x) = \alpha G_m^*(x)G_{(2k+1)m+r}^*(x) + (-1)^{m+1}(g(x))^m G_{2mk+r}^*(x).$$

This and $H(k)$ (see (11)), imply that $G_{m(2(k+1))+r}^*(x)$ equals

$$\alpha G_m^*(x)G_{(2k+1)m+r}^*(x) + (-1)^{m+1}(g(x))^m G_m^*(x)T_k(x) + (-1)^{(k+1)(m+1)}(g(x))^{m(k+1)}G_r^*(x).$$

Therefore, $G_{m(2(k+1))+r}^*(x)$ equals

$$G_m^*(x) [\alpha G_{(2k+1)m+r}^*(x) + (-1)^{m+1}(g(x))^m T_k(x)] + (-1)^{(m+1)(k+1)}(g(x))^{m(k+1)}G_r^*(x).$$

This with $T_{k+1}(x) := \alpha G_{(2k+2)m+r}^*(x) + (-1)^m(g(x))^m T_k(x)$, implies $H(k+1)$.

We finally prove part (3) by induction. Since $G_n^*(x)$ is of the Lucas type, by the Binet formula it is easy to see that $G_0(x) = 2/\alpha$. Let $S(n)$ be the statement: for every positive integer n there is a polynomial $T_n(x)$ such that $G_{2^n r}^*(x) = G_r^*(x)T_n(x) + (2/\alpha)g^{2^{n-1}r}(x)$.

Proof of $S(2)$. From part (1) we have $G_{2^2 r}^*(x) = G_{2r+2r}^*(x) = \alpha(G_{2r}^*(x))^2 - (2/\alpha)(g(x))^{2r}$. Applying again the result in part (1) for $G_{2r}^*(x)$ (and simplifying) we obtain

$$\begin{aligned} G_{2^2 r}^*(x) &= \alpha[\alpha(G_r^*(x))^2 - \frac{2}{\alpha}(-g(x))^r]^2 - \frac{2}{\alpha}(g(x))^{2r} \\ &= G_r^*(x)[\alpha^3(G_r^*(x))^3 + (-1)^{r+1}4\alpha G_r^*(x)(g(x))^r] + \frac{4}{\alpha}(g(x))^{2r} - \frac{2}{\alpha}(g(x))^{2r} \\ &= G_r^*(x)T_2(x) + \frac{2}{\alpha}(g(x))^{2r}. \end{aligned}$$

where $T_2(x) = \alpha^3(G_r^*(x))^3 + (-1)^{r+1}4\alpha G_r^*(x)(g(x))^r$. This proves $S(2)$.

We suppose that $S(k)$ is true for $k > 2$, and we prove $S(k+1)$ is true. That is, we suppose that for a fixed k there is a polynomial $T_k(x)$ such that

$$G_{2^k r}^*(x) = G_r^*(x)T_k(x) + (2/\alpha)g^{2^{k-1}r}(x).$$

From part (1) we have $G_{2^{k+1}r}^*(x) = G_{2^k r + 2^k r}^*(x) = \alpha(G_{2^k r}^*(x))^2 - (2/\alpha)(g(x))^{2^k r}$. Using the result from the inductive hypothesis $S(k)$ and simplifying, we obtain

$$\begin{aligned} G_{2^{k+1}r}^*(x) &= \alpha[G_r^*(x)T_k(x) + \frac{2}{\alpha}(g(x))^{2^{k-1}r}]^2 - \frac{2}{\alpha}(g(x))^{2^k r} \\ &= G_r^*(x)[\alpha G_r^*(x)T_k^2(x) + 4T_k(x)(g(x))^{2^{k-1}r}] + \frac{4}{\alpha}(g(x))^{2^k r} - \frac{2}{\alpha}(g(x))^{2^k r} \\ &= G_r^*(x)T_{k+1}(x) + \frac{2}{\alpha}(g(x))^{2^k r}, \end{aligned}$$

where $T_{k+1}(x) = \alpha G_r^*(x)T_k^2(x) + 4T_k(x)(g(x))^{2^{k-1}r}$. This completes the proof of part (3). \square

In the following part of this section, we present two divisibility properties for the GFP.

Proposition 8. *If $\{G'_n(x)\}$ is a GFP sequence of the Fibonacci type, then $G'_m(x)$ divides $G'_n(x)$ if and only if m divides n .*

Proof. We first prove the sufficiency. Based on the hypothesis that m divides n , there is an integer $q \geq 1$ such that $n = mq$. Then, using the Binet formula (6), we have that,

$$G'_m(x) = (a^m - b^m)/(a - b) \quad \text{and} \quad G'_{mq}(x) = (a^{mq} - b^{mq})/(a - b).$$

It is easy to see –using induction on q – that $(a^m - b^m)$ divides $(a^{mq} - b^{mq})$ which implies that $G'_m(x)$ divides $G'_{mq}(x)$. This proves the sufficiency.

We now prove the necessity. Suppose that m does not divide n and that $G'_m(x)$ divides $G'_n(x)$ for m and n greater than 1. Therefore, there integers q and r with $0 < r < n$ such that $n = mq + r$. Then by Proposition 5 part (1)

$$\begin{aligned} G'_n(x) &= G'_{mq+r}(x) \\ &= G'_{mq+1}(x)G'_r(x) + g(x)G'_{mq}(x)G'_{r-1}(x) \\ &= \left(d(x)G'_{mq}(x) + g(x)G'_{mq-1}(x)\right)G'_r(x) + g(x)G'_{mq}(x)G'_{r-1}(x) \\ &= d(x)(x)G'_{mq}(x)G'_r(x) + g(x)G'_{mq-1}(x)G'_r(x) + g(x)G'_{mq-1}(x)G'_r(x). \end{aligned}$$

Grouping terms and simplifying we obtain,

$$G'_n(x) = G'_{mq}(x)G'_{r+1}(x) + g(x)G'_{mq-1}(x)G'_r(x).$$

This and the fact that $G'_m(x) \mid G'_n(x)$ and $G'_m(x) \mid G'_{mq}(x)$ imply that

$$G'_m(x) \mid g(x)G'_{mq-1}(x)G'_r(x).$$

From Lemma 2 part (3) and Proposition 4 we know that $\gcd(G'_{mq}(x), g(x)) = 1$ and $\gcd(G'_{mq-1}(x), G'_{mq}(x)) = 1$, respectively. This implies that $G'_m(x) \mid G'_r(x)$. That is a contradiction since $\deg(G'_{r-1}(x)) < \deg(G'_{m-1}(x))$. This completes the proof. \square

Proposition 9. *Let m be a positive integer that is not a power of two. If $G_m^*(x)$ is a GFP of Lucas type, then for all odd divisors q of m , it holds that $G_{m/q}^*(x)$ divides $G_m^*(x)$. Moreover $G_{m/q}^*(x)$ is of the Lucas type.*

Proof. Let q be an odd divisor of m . If $q = 1$ the result is obvious. Let us suppose that $q \neq 1$. Therefore, there is an integer $d > 1$ such that $m = dq$. Using the Binet formula (4), where $a := a(x)$ and $b := b(x)$, we have $G_m^*(x) = G_{dq}^*(x) = (a^{dq} + b^{dq})/\alpha$. Let $X = a^d$ and $Y = b^d$. Using induction it is possible to prove that $X + Y$ divides $X^q + Y^q$. This implies that there is a polynomial $Q(x)$ such that $(X^q + Y^q)/\alpha = Q(x)(X + Y)/\alpha$. Therefore,

$$G_m^*(x) = G_{dq}^*(x) = (a^{dq} + b^{dq})/\alpha = Q(x)(a^d + b^d)/\alpha.$$

This and the Binet formula (4) imply that $G_m^*(x) = G_d^*(x)Q(x)$. \square

5 Characterization of the strong divisibility property

In this section we prove the main results of this paper. Thus, we prove the necessary and sufficient condition for the strong divisibility property for generalized Fibonacci polynomial of the Fibonacci type. We also prove that the strong divisibility property holds partially for generalized Fibonacci polynomial of the Lucas type. The other important result in this section is that the strong divisibility property holds partially for a generalized Fibonacci polynomial and its equivalent. The results here therefore provide a complete characterization of the strong divisibility property satisfied by the GFP of Fibonacci type.

We note that if $G_m^*(x)$ and $G_n^*(x)$ are two equivalent polynomial from Table 2, then $\gcd(G_m^*(x), G_n^*(x))$ is either one or $G_{\gcd(m,n)}^*(x)$. However, it is not true in general. Here we give an example of a couple GFP polynomials that do not satisfies this property. Firstly we define a Fibonacci type polynomial

$$G_0'(x) = 0, \quad G_1'(x) = 1, \quad \text{and} \quad G_n'(x) = (2x + 1)G_{n-1}'(x) + G_{n-2}'(x) \text{ for } n \geq 2.$$

We now define the equivalent polynomial of the Lucas type

$$G_0^*(x) = 2, \quad G_1^*(x) = 2x + 1, \quad \text{and} \quad G_n^*(x) = (2x + 1)G_{n-1}^*(x) + G_{n-2}^*(x) \text{ for } n \geq 2.$$

After some calculations we can see that $\gcd(G_m^*(x), G_n^*(x))$ is one, two or $G_{\gcd(m,n)}^*(x)$. Using the same polynomials we can see also that $\gcd(G_m^*(x), G_n^*(x))$ is one, two or $G_{\gcd(m,n)}^*(x)$. If we do the same calculations for numerical sequences (Fibonacci and Lucas numbers), we can see that they have the same behaviour.

In this section we use the notation $E_2(n)$ to represent the *integer exponent base two* of a positive integer n which is defined to be the largest integer k such that $2^k \mid n$.

Lemma 10. *If $R(x)$, $S(x)$ and $T(x)$ are polynomial in $\mathbb{Z}[x]$, then*

$$\gcd(R(x), T(x)) = \gcd(R(x), R(x)S(x) - T(x)).$$

Proposition 11. *Let $\{G_n^*(x)\}$ be a GFP sequence of the Lucas type. If $m \mid n$ and $E_2(n) = E_2(m)$, then $\gcd(G_n^*(x), G_m^*(x)) = G_m^*(x)$.*

Proof. First of all we recall that $E_2(n)$ is the largest integer k such that $2^k \mid n$. We suppose that $n = mq$ with $q \in \mathbb{N}$. Since $E_2(m) = E_2(n) = E_2(mq)$, we conclude that q is odd. This, Lemma 10 and Proposition 7 part (2) imply that

$$\begin{aligned} \gcd(G_n^*(x), G_m^*(x)) &= \gcd(G_{qm}^*(x), G_m^*(x)) \\ &= \gcd(G_m^*(x)T(x) + (-1)^{(n-1)m+n}(g(x))^{(n-1)m}G_m^*(x), G_m^*(x)) \\ &= G_m^*(x). \end{aligned}$$

This proves the proposition. □

Corollary 12. *Let $G_m^*(x)$ be a GFP of Lucas type. If $m > 0$ is not a power of two, then for all odd divisors q of m , it follows that $G_{m/q}^*(x)$ divides $G_m^*(x)$. More over $G_{m/q}^*(x)$ is of the Lucas type.*

Proof. It is easy to see that $E_2(m/q) = E_2(m)$. Therefore, the conclusion follows by Proposition 11. \square

Proposition 13. *Let $d_k = \gcd(G_0^*(x), G_k^*(x))$ where $G_k^*(x)$ is GFP of the Lucas type. Suppose that there is an integer $k' > 0$ such that $d_{k'} = 2$. If m is the minimum positive integer such that $d_m = 2$, then $m|n$ if and only if $d_n = 2$.*

Proof. We suppose m is the minimum positive integer such that $d_m = 2$. Suppose that $m|n$, by Proposition 11 we know that $\gcd(G_m^*(x), G_n^*(x)) = G_m^*(x)$ (we recall that $G_0^*(x) = p_0(x)$ and $|p_0(x)| = 1$ or 2). This and the fact that $2|G_m^*(x)$, implies that $\gcd(G_0^*(x), G_n^*(x)) = 2$. This proves that $d_n = 2$.

Suppose that there is $n \in \mathbb{N} - \{m\}$ that satisfies that $d_n = 2$ (note $2|\gcd(G_m^*(x), G_n^*(x))$). From the division algorithms we have that there are integer q and r such that $n = mq + r$ where $0 \leq r < m$. This and Proposition 7 part (2), imply that

$$\gcd(G_m^*(x), G_n^*(x)) = \begin{cases} \gcd(G_m^*(x), (g(x))^{(t-1)m+r} G_{m-r}^*(x)) & \text{if } q \text{ is odd;} \\ \gcd(G_m^*(x), (g(x))^{mt} G_r^*(x)) & \text{if } q \text{ is even.} \end{cases}$$

This, Lemma 2 part (3), implies that $\gcd(G_m^*(x), G_n^*(x))$ is either $\gcd(G_m^*(x), G_{m-r}^*(x))$ or $\gcd(G_m^*(x), G_r^*(x))$. From this and the fact that $2|\gcd(G_m^*(x), G_n^*(x))$, we have that $\gcd(G_r^*(x), G_0^*(x)) = 2$ or $\gcd(G_{m-r}^*(x), G_0^*(x)) = 2$. This holds only if $r = 0$, due to definition of m . Therefore, $n = mq$. \square

Lemma 14. *Let $G_k^*(x)$ be a GFP of Lucas type and let $n = mq + r$ where m, q and r are positive integers with $r < m$. If $m_1 = m - r$ when q is odd and $m_1 = r$ when q is even, then $\gcd(G_n^*(x), G_m^*(x)) = \gcd(G_{m_1}^*(x), G_m^*(x))$.*

Proof. Let

$$f(x) = \begin{cases} (-1)^{m(t-1)+t+r} (g(x))^{(t-1)m+r}, & \text{if } q \text{ is odd;} \\ (-1)^{(m+1)t} (g(x))^{mt}, & \text{if } q \text{ is even.} \end{cases}$$

This and Lemma 2 part (3) imply that $\gcd(G_m^*(x), f(x)) = 1$. Therefore, by Proposition 7 part (2) it follows that $\gcd(G_{mq+r}^*(x), G_m^*(x)) = \gcd(G_m^*(x)T(x) + f(x)G_{m_1}^*(x), G_m^*(x))$. Now it is easy to see that

$$\gcd(G_m^*(x)T(x) + f(x)G_{m_1}^*(x), G_m^*(x)) = \gcd(f(x)G_{m_1}^*(x), G_m^*(x)).$$

Since $\gcd(G_m^*(x), f(x)) = 1$, by Proposition 1 part (1) we have $\gcd(f(x)G_{m_1}^*(x), G_m^*(x)) = \gcd(G_{m_1}^*(x), G_m^*(x))$. \square

Theorem 15. *Let $\{G_n^*(x)\}$ be a GFP of the Lucas type. If m and n are positive integers and $d = \gcd(m, n)$, then*

$$\gcd(G_m^*(x), G_n^*(x)) = \begin{cases} G_d^*(x) & \text{if } E_2(m) = E_2(n); \\ \gcd(G_d^*(x), G_0^*(x)) & \text{otherwise.} \end{cases}$$

Proof. First of all we prove the result for $E_2(n) = E_2(m)$. From the Euclidean algorithm we know that there are non-negative integers q and r such that $n = mq + r$ with $r < m$. Let $d = \gcd(m, n)$. Clearly, if $r = 0$, then $d = m$. Therefore, the result holds by Proposition 11.

We suppose that $r \neq 0$. If we take m_1 as in Lemma 14, then

$$\gcd(G_n^*(x), G_m^*(x)) = \gcd(G_{mq+r}^*(x), G_m^*(x)) = \gcd(G_{m_1}^*(x), G_m^*(x)).$$

Let $M_1 = \{m, m_1\}$. Notice that $\gcd(m_1, m) = d$, $E_2(m) = E_2(m_1)$ and that $m_1 < m$. Therefore, there are non-negative integers q_1 and r_1 such that $m = m_1 q_1 + r_1$ with $r_1 < m_1$. Again, if $r_1 = 0$, by Proposition 11 we obtain that $\gcd(G_n^*(x), G_m^*(x)) = \gcd(G_m^*(x), G_{m_1}^*(x)) = G_d^*(x)$. If $r_1 \neq 0$ we repeat the previous step and then we can guarantee that

$$\gcd(G_n^*(x), G_m^*(x)) = \gcd(G_{m_1}^*(x), G_m^*(x)) = \gcd(G_{m_1}^*(x), G_{m_2}^*(x)),$$

where

$$m_2 = \begin{cases} m_1 - r_1 & \text{if } q \text{ is odd;} \\ r_1 & \text{if } q \text{ is even.} \end{cases}$$

We repeat this procedure t times until we obtain the ordered decreasing sequence $m > m_1 > m_2 > \dots > m_t \geq d$ such that $E_2(m) = E_2(m_t)$ and $\gcd(m_t, m_{t-1}) = d$, where

$$m_t = \begin{cases} m_{t-1} - r_{t-1} & \text{if } q \text{ is odd;} \\ r_{t-1} & \text{if } q \text{ is even.} \end{cases}$$

Notice that $M_t = \{m, m_1, m_2, \dots, m_t\} = M_{t-1} \cup \{m_t\}$ is an ordered set of natural numbers, therefore there is a minimum element. Since M_t is constructed with a sequence of decreasing positive integer numbers, there must be an integer k such that $M_t \subset M_k$ for all $t < k$ and M_{k+1} is undefined. Thus, the procedure ends with M_k . Note that $m > m_1 > m_2 > \dots > m_k \geq d$ such that $E_2(m) = E_2(m_k)$ and $\gcd(m_k, m_{k-1}) = d$.

Claim. The minimum element of M_k is $m_k = d$ and $m_k \mid m_{k-1}$.

Proof of claim. From the Euclidean algorithm we know that there are non-negative integers q_k and r_k such that $m_{k-1} = m_k q_k + r_k$ with $r_k < m_k$. If $r_k \neq 0$ we can repeat the procedure describe above to obtain a new set M_{k+1} with $M_k \subset M_{k+1}$. That is a contradiction. Therefore, $r_k = 0$. So, $m_{k-1} = m_k q_k$. This implies that $\gcd(m_k, m_{k-1}) = d$. Thus, $m_k = d$. This proves the claim.

The Claim and the Proposition 11 allow us to conclude that

$$\gcd(G_n^*(x), G_m^*(x)) = \gcd(G_m^*(x), G_{m_1}^*(x)) = \dots = \gcd(G_{m_{k-1}}^*(x), G_{m_k}^*(x)) = G_d^*.$$

We now prove by cases that $\gcd(G_n^*(x), G_m^*(x)) = \gcd(G_d^*(x), G_0^*(x))$ if $E_2(n) \neq E_2(m)$ and $d = \gcd(n, m)$.

Case 1. Suppose that $m < n$ and that $E_2(n) < E_2(m)$. From the Euclidean algorithm there are two non-negative integers q and r such that $n = mq + r$ with $r < m$. Let $m_1 = m - r$ when q is odd and $m_1 = r$ when q is even (as defined as in Lemma 14). Since $n = mq + r$ and $E_2(n) < E_2(m)$, we have that $r \neq 0$. It is easy to see that $E_2(n) = E_2(r)$, and therefore $E_2(n) = E_2(m_1)$. This and Lemma 14 imply that $\gcd(G_n^*(x), G_m^*(x)) = \gcd(G_m^*(x), G_{m_1}^*(x))$.

Since $E_2(m_1) = E_2(n) < E_2(m)$ and $m_1 < m$, the criteria for Case 2 are satisfied here, so the proof of this case may be completed as we are going to do in Case 2 below.

Case 2. Suppose that $E_2(m) < E_2(n)$ and that $m < n$. From the Euclidean algorithm we know that there are two non-negative integers r and q such that $n = mq + r$ with $r < m$. If $r = 0$, then q must be even (because $E_2(m) < E_2(n)$). Let $k = E_2(q)$ and we consider two subcases on k .

Subcase 1. If $k = 1$, then $q = 2t$ where t is odd. Therefore, by the Proposition 7 part (1) we have that $G_n^*(x) = G_{2mt}^*(x) = \alpha(G_{mt}^*(x))^2 + (-1)^{mt+1}(G_0^*(x))(-g(x))^{mt}$. This, Proposition 11, Lemma 2 part (3) and Lemma 10 imply that

$$\begin{aligned} \gcd(G_n^*(x), G_m^*(x)) &= \gcd(\alpha(G_{mt}^*(x))^2 + (-1)^{mt+1}G_0^*(x)(-g(x))^{mt}, G_m^*(x)) \\ &= \gcd((-1)^{mt+1}G_0^*(x)(-g(x))^{mt}, G_m^*(x)) \\ &= \gcd(G_0^*(x), G_m^*(x)) \\ &= \gcd(G_0^*(x), G_d^*(x)). \end{aligned}$$

Subcase 2. If $k > 1$, then $q = 2^k t$ where t is odd. Therefore, by the Proposition 7 part (3), there is a polynomial $T_k(x)$ such that $G_n^* = G_{2^k mt}^* = G_{mt}^*(x)T_k(x) + G_0^*(x)g^{2^{k-1}mt}(x)$. This, Proposition 11, Lemma 2 part (3) and Lemma 10 imply

$$\begin{aligned} \gcd(G_n^*(x), G_m^*(x)) &= \gcd(G_{mt}^*(x)T_k(x) + G_0^*(x)g^{2^{k-1}mt}(x), G_m^*(x)) \\ &= \gcd(G_0^*(x)g^{2^{k-1}mt}(x), G_m^*(x)) \\ &= \gcd(G_0^*(x), G_m^*(x)) \\ &= \gcd(G_0^*(x), G_d^*(x)). \end{aligned}$$

Let us now suppose that $r \neq 0$. This and Lemma 14, imply that $\gcd(G_n^*(x), G_m^*(x)) = \gcd(G_m^*(x), G_{m_1}^*(x))$, where $m_1 = m - r$ when q is odd and $m_1 = r$ when q is even (as defined as in Lemma 14). Therefore, $m_1 < m < n$ and $\gcd(m, n) = \gcd(m, m_1) = d$.

We analyze both, the case in which $m_1 \mid m$ and the case in which $m_1 \nmid m$. Suppose that $m = m_1 q_2$ and we consider two cases for q_2 .

Subcase q_2 is odd. If q_2 is odd we have that $E_2(m_1) = E_2(m)$. Therefore, by Proposition 11 we obtain that

$$\gcd(G_m^*(x), G_n^*(x)) = \gcd(G_m^*(x), G_{m_1}^*(x)) = G_d^*(x) \text{ and } E_2(G_d^*(x)) < E_2(G_n^*(x)).$$

This imply that $\gcd(G_m^*(x), G_n^*(x)) = \gcd(G_d^*(x), G_0^*(x))$.

Subcase q_2 is even. If q_2 is even, then $E_2(m_1) < E_2(m)$. Now it is easy to see that $\gcd(G_m^*(x), G_n^*(x)) = \gcd(G_{m_1}^*(x), G_0^*(x)) = \gcd(G_d^*(x), G_0^*(x))$.

Now suppose that $m_1 \nmid m$. Therefore there are two non-negative integers r_2 and q_2 such that $m = m_1 q_2 + r_2$ where $0 < r_2 < m_1$. From Lemma 14 we guarantee that we can find m_2 such that $m_2 < m_1$, $\gcd(m_1, m_2) = d$ and $\gcd(G_{m_1}^*(x), G_{m_2}^*(x)) = \gcd(G_{m_1}^*(x), G_m^*(x))$. In this form we construct a set $M_t = \{n, m, m_1, m_2, \dots, m_t\}$ where $n > m > m_1 > \dots > m_t$ such that $\gcd(m_j, m_{j-1}) = d$ and

$$\gcd(G_n^*(x), G_m^*(x)) = \gcd(G_{m_1}^*(x), G_m^*(x)) = \dots = \gcd(G_{m_j}^*(x), G_{m_{j-1}}^*(x)).$$

From Lemma 14 we know that $n > m > m_1 > \dots > m_j$ ends only if $r_j = 0$. Since $M_j = \{n, m, m_1, m_2, \dots, m_j\}$ is an ordered sequence of natural numbers, it has a minimum element m_j .

Therefore, $m_j \mid m_{j-1}$. It is easy to see that $\gcd(G_n^*(x), G_m^*(x)) = \gcd(G_{m_j}^*(x), G_{m_{j-1}}^*(x))$. This is equivalent to $\gcd(G_n^*(x), G_m^*(x)) = \gcd(G_d^*(x), G_0^*(x))$. This completes the proof. \square

Corollary 16. *Let $d_k = \gcd(G_0^*(x), G_k^*(x))$ where $G_k^*(x)$ is GFP of the Lucas type. If m and n are positive integers such that $E_2(n) \neq E_2(m)$, then*

- (1) *Suppose that there is an integer $k' > 0$ such that $d_{k'} = 2$. If r is the minimum positive integer such that $d_r = 2$, then*

$$\gcd(G_m^*(x), G_n^*(x)) = \begin{cases} 2 & \text{if } r \mid \gcd(m, n); \\ 1 & \text{otherwise.} \end{cases}$$

- (2) *If $d_k \neq 2$ for every positive integer k , then $\gcd(G_m^*(x), G_n^*(x)) = 1$.*

Proof. It is straightforward from Proposition (13). \square

Proposition 17. *Let $\{G_n^*(x)\}$ and $\{G'_n(x)\}$ be equivalent GFP. If m and n are positive integers, then*

- (1) $\gcd(G'_{m+n+1}(x), G_n^*(x)) = \gcd(G_{m+1}^*(x), G_n^*(x))$,
(2) *if $m > n$, then $\gcd(G'_{m-n+1}(x), G_n^*(x)) = \gcd(G_{m+1}^*(x), G_n^*(x))$,*
(3) *if $m < n$, then $\gcd(G'_{n-m+1}(x), G_n^*(x)) = \gcd(G_{m-1}^*(x), G_n^*(x))$.*

Proof. We first prove part (1) by induction. Let $S(n)$ be the statement (recall that $a - b = a(x) - b(x)$): for every $n \geq 1$ $\gcd((a - b)^2, G_n^*(x)) = 1$. Recall that in a GFP of Lucas type holds that $\gcd(p_0(x), p_1(x)) = \gcd(p_0(x), d(x)) = 1$ and that $2p_1(x) = p_0(x)d(x)$. From this and using Proposition 6 part (1) with $m = n = 0$, it is easy to see that $\gcd((a - b)^2, G_1^*(x)) = 1$. We now prove that $S(2)$ is also true. It is easy to see that

$$\begin{aligned} \gcd((a - b)^2, G_2^*(x)) &= \gcd(a^2(x) + b^2(x) - 2ab, G_2^*(x)) \\ &= \gcd(G_2^*(x) + 2g(x), G_2^*(x)) \\ &= \gcd(2g(x), G_2^*(x)). \end{aligned}$$

From Lemma (2) part (3) we know that $\gcd(g(x), G_2^*(x)) = 1$. This implies that either

$$\gcd((a - b)^2, G_2^*(x)) = 1 \quad \text{or} \quad \gcd((a - b)^2, G_2^*(x)) = 2.$$

If $\gcd((a - b)^2, G_2^*(x)) = 2$, then $2 \mid (d^2(x) + 4g(x))$ and $2 \mid G_2^*(x)$. So, $2 \mid d^2(x)$ and $2 \mid G_2^*(x)$. From Lemma (2) part (2) we know that $\gcd(d(x), G_2^*(x)) = 1$. This implies that $2 \nmid 1$. Therefore, $\gcd((a - b)^2, G_2^*(x)) = 1$. This proves $S(2)$.

Suppose that that $S(n)$ is true for some k . Thus, suppose that $\gcd((a - b)^2, G_k^*(x)) = 1$. We prove that $S(k + 1)$ is true. Suppose that $\gcd((a - b)^2, G_{k+1}^*(x)) = r(x)$. Therefore,

$r(x) \mid (a-b)^2$ and $r(x) \mid G_{k+1}^*(x)$. So, $r(x) \mid [(a-b)^2 G_{2k+1}'(x) - \alpha^2 (G_{k+1}^*(x))^2]$. From Proposition 6 part (1) we know that if $m = n = k$, then

$$(a-b)^2 G_{k+k+1}'(x) = \alpha^2 G_{k+1}^*(x) G_{k+1}^*(x) + \alpha^2 g(x) G_k^*(x) G_k^*(x).$$

Thus, $(a-b)^2 G_{2k+1}'(x) - \alpha^2 (G_{k+1}^*(x))^2 = \alpha^2 g(x) (G_k^*(x))^2$. This implies that $r(x)$ divides $\alpha^2 g(x) (G_k^*(x))^2$. Since $|\alpha| = 1$ or 2 , from the definition of GFP and Proposition 4 is easy to see that $\gcd(\alpha, g(x)) = 1$. We know that $\gcd(\alpha, G_n) = 1$ for every n . So, $\gcd(\alpha, r(x)) = 1$. We recall that from Lemma (2) part (3), that $\gcd(g(x), G_{k+1}^*(x)) = 1$. This and $r(x) \mid G_{k+1}^*(x)$ imply that $\gcd(r(x), g(x)) = 1$. Now it is easy to see that $r(x) \mid (G_k^*(x))^2$. Since $r(x) \mid (a-b)^2$ and $\gcd((a-b)^2, G_k^*(x)) = 1$, we have that $r(x) = 1$. This proves that $S(k+1)$ is true. That is, $\gcd((a-b)^2, G_n^*(x)) = 1$.

We now prove that $\gcd(G_{m+n+1}'(x), G_n^*(x)) = \gcd(G_{m+1}^*(x), G_n^*(x))$. Proposition 6 part (1), implies that

$$\begin{aligned} \gcd((a-b)^2 G_{m+n+1}'(x), G_n^*(x)) &= \gcd(\alpha^2 G_{m+1}^*(x) G_{n+1}^*(x) + \alpha^2 g(x) G_m^*(x) G_n^*(x), G_n^*(x)) \\ &= \gcd(\alpha^2 G_{m+1}^*(x) G_{n+1}^*(x), G_n^*(x)). \end{aligned}$$

From Proposition 4 and $\gcd(\alpha, G_{n+1}) = 1$ we know that $\gcd(\alpha^2 G_{n+1}^*(x), G_n^*(x)) = 1$. Therefore, by Proposition 1 part (2) we have $\gcd(G_{m+1}^*(x) G_{n+1}^*(x), G_n^*(x)) = \gcd(G_{m+1}^*(x), G_n^*(x))$. This implies that

$$\gcd((a-b)^2 G_{m+n+1}'(x), G_n^*(x)) = \gcd(G_{m+1}^*(x), G_n^*(x)).$$

This and $\gcd((a-b)^2, G_n^*(x)) = 1$ imply that

$$\gcd(G_{m+n+1}'(x), G_n^*(x)) = \gcd(G_{m+1}^*(x), G_n^*(x)).$$

Proof of part (2). From Lemma 2 part (3) it is easy to see that $\gcd(G_{m-n+1}'(x), G_n^*(x))$ is equal to $\gcd((g(x))^n G_{m+1-n}'(x), G_n^*(x))$. This and Proposition 5 part (2) (after interchanging the roles of m and n), imply that $\gcd(G_{m-n+1}'(x), G_n^*(x))$ equals

$$\gcd(\alpha G_{m+1}'(x) G_n^*(x) - G_{m+1+n}'(x), G_n^*(x)) = \gcd(G_{m+n+1}'(x), G_n^*(x)).$$

The conclusion follows from part (1).

Proof of part (3). From Lemma 2 part (3) it is easy to see that

$$\gcd(G_{n-m+1}'(x), G_n^*(x)) = \gcd((-g(x))^{m-1} G_{n-(m-1)}'(x), G_n^*(x)).$$

This and Proposition 5 part (3), imply that $\gcd(G_{m-n+1}'(x), G_n^*(x))$ equals

$$\gcd(G_{n+m-1}'(x) - \alpha G_{m-1}'(x) G_n^*(x), G_n^*(x)) = \gcd(G_{n+(m-2)+1}'(x), G_n^*(x)).$$

The conclusion follows from part (1). \square

Theorem 18. Let $\{G_n^*(x)\}$ and $\{G_n'(x)\}$ be equivalent GFP. If m and n are positive integers and $\gcd(m, n) = d$, then

$$\gcd(G_m'(x), G_n^*(x)) = \begin{cases} G_d^*(x) & \text{if } E_2(m) > E_2(n); \\ \gcd(G_d^*(x), G_0^*(x)) & \text{otherwise.} \end{cases}$$

Proof. We suppose that $E_2(m) > E_2(n)$. We prove this part of the Theorem by cases.

Case $m > n$. Since $m > n$, there is a positive integer l such that $m = n + l$. Therefore, $\gcd(G'_m(x), G_n^*(x)) = \gcd(G'_{l-1+n+1}(x), G_n^*(x))$. This and Proposition 17 part (1) imply that $\gcd(G'_m(x), G_n^*(x)) = \gcd(G_l^*(x), G_n^*(x))$. Since $E_2(m) > E_2(n)$ and $m = n + l$, we have that $E_2(l) = E_2(n)$. This and Theorem 15 imply that $\gcd(G_l^*(x), G_n^*(x)) = G_{\gcd(l,n)}^*(x)$. From Lemma 10 it is easy to see that $\gcd(l, n) = \gcd(m, n)$. Thus, $\gcd(G'_m(x), G_n^*(x)) = G_{\gcd(m,n)}^*(x)$. So, $\gcd(G'_m(x), G_n^*(x)) = G_{\gcd(m,n)}^*(x)$.

Case $m < n$. The proof of this case is similar to the proof of Case $m > n$. It is enough to replace m by $n - (l + 1)$ in $\gcd(G'_m(x), G_n^*(x))$, and then use Proposition 17 part (3).

We now suppose that $E_2(m) \leq E_2(n)$. We prove this part of the Theorem by cases.

Case $m > n$. So, there is a positive integer l such that $m = l + n$. Therefore by Proposition 17 part (1) we have

$$\gcd(G'_m(x), G_n^*(x)) = \gcd(G'_{n+(l-1)+1}(x), G_n^*(x)) = \gcd(G_l^*(x), G_n^*(x)).$$

Note that if $m = n + l$ and $E_2(m) \leq E_2(n)$, then there are integers k_1, k_2, q_1 and q_2 with $k_1 \leq k_2$ such that $m = 2^{k_1}q_1$ and $n = 2^{k_2}q_2$. Since $m = n + l$, we see that $E_2(l) \neq E_2(n)$. This and Theorem 15 imply that $\gcd(G'_m(x), G_n^*(x)) = \gcd(G_0^*(x), G_{\gcd(n,l)}^*(x))$. Thus, $\gcd(G'_m(x), G_n^*(x)) = \gcd(G_0^*(x), G_{\gcd(m,n)}^*(x))$.

Case $m < n$. The proof of this case is similar to the proof of Case $m > n$. It is enough to replace m by $n - (l + 1) + 1$ in $\gcd(G'_m(x), G_n^*(x))$, and then use Proposition 17 part (3).

Case $m = n$. Since $n = (2n - 1) - n + 1$, taking $m = 2n - 1$ in Proposition 17 part (2) and using Theorem 15 we obtain that

$$\gcd(G'_n(x), G_n^*(x)) = \gcd(G'_{(2n-1)-n+1}(x), G_n^*(x)) = \gcd(G_{2n}^*(x), G_n^*(x)) = \gcd(G_0^*(x), G_n^*(x)).$$

This completes the proof. \square

Hoggatt and Bicknell-Johnson [10, Thm. 3.4] proved that Fibonacci polynomials, Chebyshev polynomials of second kind, Morgan-Voyce polynomial, and Schechter polynomial satisfy the strong divisibility property. Theorem 19 proves the necessary and sufficient condition for the polynomials in a generalized Fibonacci polynomial sequence to satisfy the strong divisibility property. Norfleet [22] also prove the some strong divisibility property for GFP of Fibonacci type.

Theorem 19. *Let $\{G_k(x)\}$ be a GFP of either Fibonacci type or Lucas type. For any two positive integers m and n it holds that $\gcd(G_m(x), G_n(x)) = G_{\gcd(m,n)}(x)$ if and only if $\{G_k(x)\}$ is a sequence of GFP of the Fibonacci type.*

Proof. Let $\{G'_n(x)\}$ be a generalized Fibonacci polynomial sequence of the Fibonacci type, we now show that $\gcd(G'_m(x), G'_n(x))$ divides $G'_{\gcd(m,n)}(x)$ for $m > 0, n > 0$ and vice versa.

If G'_n is of Fibonacci type, by Proposition 8, it is clear that $G'_{\gcd(m,n)} \mid \gcd(G'_m(x), G'_n(x))$. Next we show that $\gcd(G'_m(x), G'_n(x))$ divides $G'_{\gcd(m,n)}$.

Let $k = \gcd(m, n)$ and suppose without lost of generality that k is neither equal n nor equal m . The Bézout identity implies that there are two positive integers r and s such that

$k = rm - sn$. So, $rm = k + sn$ and $G'_{rm}(x) = G'_{k+sn}(x)$. This, Proposition 5 part (1), and the fact that $k + sn = (k + (sn - 1)) + 1$, imply that

$$G'_{rm}(x) = G'_{k+1}(x)G'_{s'n}(x) + g(x)G'_k(x)G'_{sn-1}(x).$$

We note that, by Proposition 8, $G'_m(x)$ divides $G'_{rm}(x)$ and $G'_n(x)$ divides $G'_{sn}(x)$. Since $\gcd(G'_m(x), G'_n(x)) \mid G'_m(x)$ and $\gcd(G'_m(x), G'_n(x)) \mid G'_n(x)$, and $G'_m(x) \mid G'_{rm}(x)$ and $G'_n(x) \mid G'_{s'n}(x)$, we have that $\gcd(G'_m(x), G'_n(x))$ divides $G'_{rm}(x)$ and $G'_{s'n}(x)$. This together with Lemma 2 part (3) and the fact that $\gcd(G'_m(x), G'_n(x))$ does not divide $G'_{s'n-1}(x)$, implies that $\gcd(G'_m(x), G'_n(x))$ divides $G'_k(x)$.

Conversely, suppose that $\{G_n(x)\}$ is a generalized Fibonacci polynomial sequence such that the strong divisibility property holds, or $\gcd(G_m(x), G_n(x)) = G_{\gcd(m,n)}(x)$ for any two positive integers m and n , we now show that both $G_m(x)$ and $G_n(x)$ are GFP of the Fibonacci type. We prove this using the method of contradiction.

If $G_m(x)$ and $G_n(x)$ are in $\{G_n(x)\}$ such that they are both GFP of the Lucas type, then by Theorem 15 we obtain a contradiction. This completes the proof. \square

6 The gcd properties of Familiar GFP and questions

In this section we formulate a general question and present three tables which are corollaries of the main results in Section 5. These tables give us the strong divisibility property of the familiar polynomials which satisfy the Binet formulas (4) and (6). Table 3 gives the gcd's for Fibonacci polynomials, Pell polynomials, Fermat polynomials, Jacobsthal polynomials, Chebyshev's second kind polynomials and one type of Morgan-Voyce B_n polynomials. Table 4 gives the strong divisibility property of the Lucas polynomials, Pell-Lucas polynomials, Fermat-Lucas polynomials, Jacobsthal-Lucas polynomials, Chebyshev's first kind polynomials and Morgan-Voyce C_n polynomials, while Table 5 gives the gcd of a polynomial of the Lucas type and its equivalent.

We should note here that in the case of Table 4, the strong divisibility property is partially satisfied since it only holds when the largest powers of 2 that divides m and the largest powers of 2 that divides n are both equal. (That is, $E_2(m) = E_2(n)$.) Similarly the strong divisibility property only holds in Table 5 when $E_2(n) < E_2(m)$.

Polynomial	The Fibonacci gcd property
Fibonacci	$\gcd(F_m(x), F_n(x)) = F_{\gcd(m,n)}(x)$
Pell	$\gcd(P_m(x), P_n(x)) = P_{\gcd(m,n)}(x)$
Fermat	$\gcd(\Phi_m(x), \Phi_n(x)) = \Phi_{\gcd(m,n)}(x)$
Chebyshev second kind	$\gcd(U_m(x), U_n(x)) = U_{\gcd(m,n)}(x)$
Jacobsthal	$\gcd(J_m(x), J_n(x)) = J_{\gcd(m,n)}(x)$
Morgan-Voyce	$\gcd(B_m(x), B_n(x)) = B_{\gcd(m,n)}(x)$

Table 3: Strong divisibility property of polynomials Fibonacci type.

Polynomial	Case 1: $E_2(m) = E_2(n)$	Case 2: $E_2(m) \neq E_2(n)$
Lucas	$\gcd(D_m(x), D_n(x)) = D_{\gcd(m,n)}(x)$	$\gcd(D_m(x), D_n(x)) = 1$
Pell-Lucas-prime	$\gcd(Q'_m(x), Q'_n(x)) = Q'_{\gcd(m,n)}(x)$	$\gcd(Q'_m(x), Q'_n(x)) = 1$
Fermat-Lucas	$\gcd(\vartheta_m(x), \vartheta_n(x)) = \vartheta_{\gcd(m,n)}(x)$	$\gcd(\vartheta_m(x), \vartheta_n(x)) = 1$
Chebyshev first kind	$\gcd(T_m(x), T_n(x)) = T_{\gcd(m,n)}(x)$	$\gcd(T_m(x), T_n(x)) = 1$
Jacobsthal-Lucas	$\gcd(Q_m(x), Q_n(x)) = Q_{\gcd(m,n)}(x)$	$\gcd(Q_m(x), Q_n(x)) = 1$
Morgan-Voyce	$\gcd(C_m(x), C_n(x)) = C_{\gcd(m,n)}(x)$	$\gcd(C_m(x), C_n(x)) = 1$

Table 4: Strong divisibility property (partially) of polynomials of Lucas type.

Polynomials	$E_2(n) < E_2(m)$	Otherwise
Fibonacci, Lucas	$\gcd(F_m(x), D_n(x)) = D_d(x)$	$\gcd(F_m(x), D_n(x)) = 1$
Pell, Pell-Lucas-prime	$\gcd(P_m(x), Q'_n(x)) = Q'_d(x)$	$\gcd(P_m(x), Q'_n(x)) = 1$
Fermat, Fermat-Lucas	$\gcd(\Phi_m(x), \vartheta_n(x)) = \vartheta_d(x)$	$\gcd(\Phi_m(x), \vartheta_n(x)) = 1$
Chebyshev both kinds	$\gcd(U_m(x), T_n(x)) = T_d(x)$	$\gcd(U_m(x), T_n(x)) = 1$
Jacobsthal, Jacobsthal-Lucas	$\gcd(J_m(x), j_n(x)) = j_d(x)$	$\gcd(J_m(x), j_n(x)) = 1$
Morgan-Voyce both types	$\gcd(B_m(x), C_n(x)) = C_d(x)$	$\gcd(B_m(x), C_n(x)) = 1$

Table 5: Strong divisibility property (partially) of polynomials of Lucas type and their equivalents, where $d = \gcd(m, n)$.

6.1 Questions

1. Let $\{G_n^*(x)\}$ and $\{S_n(x)\}$ be generalized Fibonacci polynomial sequences of Lucas type and Fibonacci type, respectively. If $S_n(x)$ is not the equivalent of $G_n^*(x)$, what is the $\gcd(G_k^*(x), S_m(x))$? We believe that the answer is: 1 or x .
2. Let $\{G_n(x)\}$ and $\{S_n(x)\}$ be two different Fibonacci polynomial sequences of the same type, then do they satisfy the strong divisibility property?
3. (**Conjecture.**) The GFP T_n and S_m satisfy the strong divisibility property if and only if T_n and S_m are both of Fibonacci type and they belong to the same generalized Fibonacci polynomial sequence. Theorems 18 and 19 are evidence that the conjecture is true.
4. Let \mathcal{R} be a set of recursive functions. If $\mathcal{F} : \mathbb{N} \rightarrow \mathcal{R}$, $\mathcal{G} : \mathcal{R} \times \mathcal{R} \rightarrow \mathcal{R}$ and $g : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$, under what conditions $\mathcal{G} \circ (\mathcal{F} \times \mathcal{F}) = \mathcal{F} \circ g$ for all $\mathcal{F} \in \mathcal{R}$ and a fix g ?

7 Acknowledgement

The first and last authors were partially supported by The Citadel Foundation.

References

- [1] R. André-Jeannin, Differential properties of a general class of polynomials, *Fibonacci Quart.* **33** (1995), 453–458.
- [2] R. André-Jeannin, A generalization of Morgan-Voyce polynomials, *Fibonacci Quart.* **32** (1994), 228–231.
- [3] R. Flórez, R. Higuita and A. Mukherjee, Alternating sums in the Hosoya polynomial triangle, *J. Integer Seq.*, **17** (2014), Article 14.9.5.
- [4] R. Flórez, R. Higuita and L. Junes, 9-modularity and gcd properties of generalized Fibonacci numbers, *Integers*, **14** (2014), Paper No. A55, 14pp.
- [5] R. Flórez and L. Junes, gcd properties in Hosoya’s triangle, *Fibonacci Quart.* **50** (2012), 163–174.
- [6] M. Hall, Divisibility Sequences of Third Order, *Amer. J. Math.* **58** (1936), 577–584.
- [7] R. T. Hansen, Generating Identities for Fibonacci and Lucas Triples , *Fibonacci Quart.* **10** (1972), 571–578.
- [8] P. Hilton, P. J. Pedersen, and L. Vrancken, On certain arithmetic properties of Fibonacci and Lucas numbers, *Fibonacci Quart.* **3** (1995), 211–217.
- [9] V. E. Hoggatt, Jr., and C. T. Long, Divisibility properties of generalized Fibonacci polynomials, *Fibonacci Quart.* **12** (1974), 113–120.
- [10] V. E. Hoggatt, Jr., and M. Bicknell-Johnson, Divisibility properties of polynomials in Pascal’s triangle, *Fibonacci Quart.* **16** (1978), 501–513.
- [11] A. F. Horadam, A synthesis of certain polynomial sequences, *Applications of Fibonacci numbers*, Vol. 6 (Pullman, WA, 1994), 215–229, Kluwer Acad. Publ., Dordrecht, 1996.
- [12] C. Kimberling, , Greatest common divisors of sums and differences of Fibonacci, Lucas, and Chebyshev polynomials, *Fibonacci Quart.* **17** (1979), 18–22.
- [13] C. Kimberling, Strong divisibility sequences and some conjectures, *Fibonacci Quart.* **17** (1979), 13–17.
- [14] C. Kimberling, Strong divisibility sequences with nonzero initial term, *Fibonacci Quart.* **16** (1978), 541–544.
- [15] E. Lucas, Théorie des fonctions numériques simplement périodiques, *Amer. J. Math.* **1** (1878), 184–240, 289–321.
- [16] A. F. Horadam and J. M. Mahon, Pell and Pell-Lucas polynomials, *Fibonacci Quart.* **23** (1985), 7–20.

- [17] A. F. Horadam, Chebyshev and Fermat polynomials for diagonal functions, *Fibonacci Quart.* **17** (1979), 328–333.
- [18] T. Koshy, *Fibonacci and Lucas Numbers with Applications*, John Wiley, New York, 2001.
- [19] J. Lahr, Fibonacci and Lucas numbers and the Morgan-Voyce polynomials in ladder networks and in electric line theory, *Fibonacci numbers and their applications*, (Patras, 1984), 141–161.
- [20] W. McDaniel, The g.c.d. in Lucas sequences and Lehmer number sequences, *Fibonacci Quart.* **29** (1991), 24–29.
- [21] A. M. Morgan-Voyce, Ladder network analysis using Fibonacci numbers, *IRE Trans. Circuit Th.* **CT-6** (1959), 321–322.
- [22] M. Norfleet, Characterization of second-order strong divisibility sequences of polynomials, *Fibonacci Quart.* **43** (2005), 166–169.
- [23] M. O. Rayes, V. Trevisan, and P. S. Wang, Factorization properties of Chebyshev polynomials, *Comput. Math. Appl.* **50** (2005), 1231–1240.
- [24] M. N. S. Swamy, Properties of the polynomials defined by Morgan-Voyce, *Fibonacci Quart.* **4** (1966a), 73–81.
- [25] M. Ward, Note on divisibility sequences, *Bull. Amer. Math. Soc.* **42** (1936), 843–845.
- [26] W. A. Webb and E. A. Parberry, Divisibility properties of Fibonacci polynomials, *Fibonacci Quart.* **7** (1969), 457–463.

MSC 2010: Primary 11B39; Secondary 11B83.

Keywords: Greatest common divisor, strong divisibility property, generalized Fibonacci polynomial, Fibonacci polynomial, Lucas polynomial.